IN THE SPECIFICATION

Please amend paragraph 8 on page 8 as follows:

- randomly picking challenge parameters $r_i \in G$ and $a_{ij} \in Z_d$ for i = 1, … , k and j = 1, … , s+t (the number of input elements is now extended to s+t) and computing a challenge value $u_i = dr_i + a_{i1}g_1 + \ldots a_{is}g_s + a_{is+1}[[y]]\underline{x}_1 + \ldots + a_{is+t}[[y]]\underline{x}_t$,